Cryptacus Newsletter

March'17 Cryptacus Newsletter

Welcome to the latest edition of the monthly Cryptacus.eu newsletter, bringing you a glimpse into recent developments in the IoT cryptanalysis area. We'd love to receive more of your contributions, comments & feedback at cryptacus.newsletter@irisa.fr

News from the Chair

by GILDAS AVOINE

Dear Cryptacus Members,

We will have in March the first Cryptacus' workshop, which will take place in Sutomore, Montenegro, on March 14-15th.

A call for presentations was published, and 14 presentation proposals were accepted. This is the list of accepted speakers:

- David Gerault
- Orhun Kara
- Sinisa Tomovic
- Darren Hurley-Smith
- Cesar Garcia
- Davide Bellizia
- Constantinos Patsakis
- Thomas Gougeon
- Ziya Alper Genc
- Eleni Isa
- Pietro Monsurro
- Nicola Tuveri
- Miodrag Mihaljevic

If not done yet, you can still register in the workshop using this link: `https://goo.gl/XRMOVH`

Note that booking in the hotel of the workshop is convenient because the organise negociated that the room rate will include both the costs of transportation from/to the airport and the lunches. If you have questions, do not hesitate to directly contact Milena.

The end of the Grant Period is also coming soon, i.e., at the end of April. As usual, Short-Term Scientific Missions (STSM) can not be organized over two Grant Periods. However, candidates interested by STSMs can already apply for research stays starting in June.

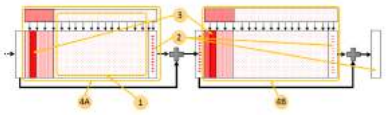
The Management Committee will also have a meeting in Montenegro in order to define the activities that will be organized during the next Grant Period.

If you have ideas, wishes, or if you want to organize an event, do not hesitate to contact either the MC Chair or the Vice-chair, Gildas Avoine and Julio Hernandez-Castro, respectively, or any Working Group leader or vice-leader.

See you in Sutomore!

Gildas

Recommended reading



There is no way that you have not heard of the news that a first SHA-1 collision has been found, but we have to honor here the important

news and the relevance of the finding, that although totally expected has still considerable impact.

The new was announced at the Google Security Blog on the 23^{rd} of February (at `https://goo.gl/B4v3a0`). It was a nice joint effort by a team of CWI researchers (Marc Stevens, Pierre Karpman) and Google engineers (Elie Bursztein, Ange Albertini, Yarik Markov, Alex Petit, Clement Baisse).

They spent a computation effort equivalent to $2^{63.1}$ SHA-1 compressions (see https://eprint.iacr.org/2017/190).

As the authors write, the computation took "approximately 6,500 CPU years and 100 GPU years. As a result while the computational power spent on this collision is larger than other public cryptanalytic computations, it is still more than 100,000 times faster than a brute force search."

Despite the undeniably importance of the result, it created some funny responses on different social networks, such as:

The authors added: "Moving forward, it's more urgent than ever for security practitioners to migrate to safer cryptographic hashes such as SHA-256 and SHA-3. Following Google's vulnerability disclosure policy, we will wait 90 days before releasing code that allows anyone to create a pair of PDFs that hash to the same SHA-1 sum given two distinct images with some pre-conditions."

More info in 90 days, and at `https://shattered.io/`

Funding News

We will arrange in the next Cryptacus meeting in Montenegro for a slot to discuss some of these calls in detail and will plan ahead for them, focusing particularly on the August calls as by them the April one will be too close. Our aim is to facilitate the build up of consortia to successfully apply to several of these opportunities.

If you are interested in participating in this session, and particularly if you want to briefly present a project idea to get feedback and potentially start building-up a consortium, please contact me for booking a slot.

I haven't been contacted by anyone so far, so please hurry up if you want to contribute to this.

In addition, but only if anyone shows interest, we will discuss Marie Curie mobility grants as well.

Last but not least, though it may be a little late for most of you reading the newsletter, there is an interesting event in coming up very soon.

It's the Horizon 2020 Secure Societies European Info Day and Brokerage Event, that will take place in Brussels on 6 - 7 March at the Radisson Blu Royal Hotel.

The event is "organized by the Network of Secure Societies National Contact Points - SEREN3, in collaboration with the European Commission. This information day and brokerage event gives details on the calls for proposals H2020-CIP 2017, H2020-SEC 2017 and H2020-DS-2017" and is highly recommended.

There will be at least 265 participants, and there is the possibility to arrange short meetings with up to 6 of them to discuss ideas and consortium building.

If it's too late for you to register, keep an eye for similar events later this year. We will inform you of them in here.

More info at `https://www.b2match.eu/seren3brussels2017`

Open Positions

Please send us any employment opportunity you want to publicize in the newsletter.

There are plenty of interesting open positions, such as:

- Professor in Cryptology at Aalto University. Deadline is the 01/04/2017. More info at `https://goo.gl/7hy5GL`
- Professorship in Computer Networks and Communication Systems at Brandenburg University of Technology (BTU). They mention their interest in the areas of "the internet of things" and "security in computer networks". The application dead-

line is the 06/04/2017. German and English fluency required. More info at `https://www.b-tu.de/fakultaet1/`.

- Assistant Professor in Advanced Computer Science at Universiteit Leiden. Deadline is 12/03/2017. The want to appoint one assistant professor in the area of Security and another in the field of Correctness & Automated testing. Salary range from €3,427 €5,330 gross per month. More info at `https://goo.gl/1GbhN6`.

In addition, a good number of positions in the other side of the channel have recently opened or are about to close:

- Lecturer/SL/Reader in Cyber Security at the School of Computing Science, University of Glasgow. Another full time, permanent position with a salary range between £33,943 and £55,998 per annum. Deadline is the 3^{rd} of February. More info at `https://goo.gl/ioChFq`.

- Lecturer in Information Security at the Information Security Group of Royal Holloway, University of London. Deadline is the 9^{th} of April, and the salary £41,458 to £49,059 per annum. Needless to say, this is the largest information security group in the UK, and one of the most prestigious. More info at `https://goo.gl/0YZzp2`. They also offer `https://goo.gl/hWCgvY` a more teaching-focused position at the same Lecturer level.

- Lecturer in Computer Security at the School of Computer Science, within the College of Engineering and Physical Sciences of the University of Birmingham. Deadline for applications is the 2^{nd} of April. Salary range is £39,324 to £52,793, for a full time, permanent position. Birmingham has a much smaller security group but they have some very talented people and have recently recruited very well and continue to attract talent. Also one of the very top security groups in the UK. For applying, check `https://goo.gl/yDLQS9`.

- Lecturer in Cyber Security, at the University of Southampton. Application deadline is the 13^{th} March, and salary range is £37,075 to £46,924. Full-time, permanent position, more info at `https://goo.gl/gvl0qo`.

For other interesting positions all across Europe, please check the recently revamped "Researchers in Motion" portal `https://euraxess.ec.europa.eu/`.

Proposals for STSMs

By now, you should be already familiar with what Short Term Scientific Missions (or STSMs, for short) are, but we have a healthy budget for them within the Cryptacus project and not enough demand.

Until somebody sends more proposals, we will repeat the STSM offers of the past, including that of Aurélien Francillon and mine.

- "At Eurecom we are actively working on analyzing embedded devices software and building methodologies and tools for this. An example of that is ourvopen source Avatar Framework (see `http://s3.eurecom.fr/tools/avatar/`) which is aimed to reverse engineer devices and search for vulnerabilities. We are happy to receive visitors interested in the topic, for example to get help to start using the Avatar framework on a given device."

- I will be happy to receive anyone interested in investigating the many limitations and pitfalls of the PRNGs and the TRNGs currently in use on IoT devices.

Blogs and posts to read

This month, to continue with the SHA-1 theme, we will recommend the read of a blog post that can be found at `https://goo.gl/gk5AJZ` and is title "Lessons From The History Of Attacks On Secure Hash Functions" where the people of z-cash write very authoritatively about the history if hash functions.

In particular, they summarize "The main result is that there is a big gap between the history of collision attacks and pre-image attacks. Almost all older secure hash functions have fallen to collision attacks. Almost none have ever fallen to pre-image attacks.

Secondarily, no new secure hash functions (designed after approximately the year 2000) have so far succumbed to collision attacks, either."

Good read, very insightful though controversial at times.

Event calendar

Of course, the main dish in our event calendar is the next Cryptacus Management Committee & Workshop in March, 14-15th, in Sutomore, Montenegro. It will be organised by Milena Djukanovic.

Euro S&P is this year in Paris, 26-28 April. A must! More at `https://goo.gl/fvjBVN`

The summer school on real-world crypto and privacy organised by Lejla will take place in Sibenik (Croatia), June 5 to 9. Highly recommended, for all ages! Registration will open early February 2017. More relevant info at `https://goo.gl/cSCcUZ`.

Even earlier on, we have (thanks Stefan!) the first spring school on security and correctness in IoT, which takes place May 8-12 in Graz, Austria. Topics range from software exploits and hardware side-channels to formal methods for security verification. Standard registration is open until April 16. More info at `http://springschool.iaik.tugraz.at/`.

The program is very interesting, and brings in some of the best in the area (including many Cryptacus people) and lots of practical labs. In addition, they offer a limited number of student stipends to cover registration.

ESORICS is this year in beautiful Oslo, from 11-15 September. Submission deadline is April 19^{th}. Hope to see many of you there!

Last but not least, Agusti Solanas is editing an Special Issue in the International Journal of RF Technologies Research and Applications (ISSN: 1754-5730) on 'Advances in RFID for Smart Cities' with a deadline of 17^{th} March and a publication date in September. More info at `https://goo.gl/YbjggH`

Agusti is also organising a special session in a IEEE Conference on Smart Health with many topics of interest for Cryptacus members, including: Security, privacy and trust management for Smart Healthcare services/applications, Lightweight cryptography for Smart Healthcare devices and systems and Cryptanalysis of protocols for Smart Healthcare devices. More info at `http://rtsi2017.ieeesezioneitalia.it/tech_sessSH.html`

See you all very soon!

Best,
Julio Hernandez-Castro